PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-306401
(43)Date of publication of application : 02.11.2001

(51)Int.Cl. G06F 12/14
G06K 17/00
G06K 19/07
G06K 19/10
G09C 1/00
H04L 9/08
H04L 9/10
H04L 9/32

(21)Application number : 2001-004730
(22)Date of filing : 12.01.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : SHIBATA OSAMU
YUGAWA YASUHEI
SEKIBE TSUTOMU
HIROTA TERUTO
SAITO YOSHIYUKI
OTAKE TOSHIHIKO

(30)Priority
Priority number : 2000006989 Priority date : 14.01.2000 Priority country : JP
2000041317 18.02.2000 JP

(54) AUTHENTICATION COMMUNICATION DEVICE AND ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an access device capable of preventing information for accessing a secret data storage area from being leaked.
SOLUTION: An access device transmits disturbed access information generated by disturbing access information indicating the secret data storage area to a recording medium to certificate the validity of the recording medium by a challenge response type certification protocol. The recording medium certifies the validity of the access device. When the validity of both the recording medium and access device is certified, the recording medium separates the access information from the transmitted disturbed access information and the access device reads out digital information from an area indicated by the separated access information or writes the digital information in the area indicated by the access information.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is the authentication communication system which consists of a record medium which has the field which memorizes digital information, and access equipment which writes digital information in digital information read-out or said field from said field. By transmitting the disturbance-ized access information which disturbed and generated the access information which shows said field from said

access equipment to said record medium The 1st authentication phase when said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication phase when said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment Authentication communication system characterized by including the transfer phase which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.

[Claim 2] In said 1st authentication phase said access equipment The access information acquisition section which acquires the access information which shows said field, and the random-number acquisition section which acquires a random number, The generation section which compounds said acquired access information and the acquired random number, and generates random-number-ized access information, The cryptopart which gives cryptographic algorithm to the generated random-number-ized access information, and generates disturbance-ized access information is included. Said record medium Said access equipment is authentication communication system according to claim 1 characterized by including the authentication section which attests justification of said record medium using said generated response value including the response value generation section which generates a response value from the generated disturbance-ized access information.

[Claim 3] It is the authentication communication system according to claim 2 characterized by including the decode section which gives a decode algorithm to the disturbance-ized access information by which said record medium was generated in said transfer phase, and generates random-number-ized access information, and the separation section which separates access information from the transmitted random-number-ized access information.

[Claim 4] Said random-number acquisition section is authentication communication system according to claim 3 characterized by acquiring a random number including the random-number kind storage section said access equipment has remembered the random-number kind to be further in said 1st authentication phase by reading a random-number kind from the random-number kind storage section.

[Claim 5] It is the authentication communication system according to claim 4 characterized by for said access equipment using said disturbance-ized access information as a random-number kind further in said 1st authentication phase, and overwriting said random-number kind storage section.

[Claim 6] the authentication communication system according to claim 3 characterized by for said random-number acquisition section to acquire a random number in said 1st authentication phase including the random-number kind storage

section said access equipment has remembered the random-number kind to be further by generating a random number based on the random-number kind which carried out reading appearance of the random-number kind, and carried out reading appearance from the random-number kind storage section.

[Claim 7] It is the authentication communication system according to claim 6 characterized by overwriting said random-number kind storage section by using as a random-number kind said random number with which said access equipment was further generated in said 1st authentication phase.

[Claim 8] In said transfer phase, the record medium which is recording digital information on said field Digital information is read from said field shown by said access information. Said access equipment which reads digital information from said field including the cryptopart which gives cryptographic algorithm to the read digital information and generates encryption digital information Said decode algorithm is authentication communication system according to claim 3 characterized by decoding the cipher generated by said cryptographic algorithm including the decode section which gives a decode algorithm to the generated encryption digital information, and generates DESHITARU information.

[Claim 9] In said transfer phase, said access equipment which writes digital information in said field The digital information acquisition section which acquires digital information, and the cryptopart which gives cryptographic algorithm to the acquired digital information and generates encryption DESHITARU information are included. Said record medium Give a decode algorithm to said generated encryption digital information, and digital information is generated. Said decode algorithm is authentication communication system according to claim 3 characterized by decoding the cipher generated by said cryptographic algorithm including the decode section which writes digital information in said field shown by said access information.

[Claim 10] In said transfer phase, said access equipment which writes digital information in said field The digital information acquisition section which acquires digital information, and the contents key acquisition section which acquires a contents key, The 1st cryptopart which gives the 1st cryptographic algorithm to the acquired contents key, and generates an encryption contents key, The 2nd encryption section which gives the 2nd cryptographic algorithm to said generated encryption contents key, and generates a duplex encryption contents key, The 3rd cryptopart which gives the 2nd cryptographic algorithm to said acquired digital information using said contents key, and generates encryption DESHITARU information is included. Said record medium Give the 1st decode algorithm to said generated duplex encryption contents key, and an encryption contents key is generated. Said record medium is authentication communication system according to claim 3 characterized by including the field which memorizes said generated encryption digital information further including the decode section which writes an encryption contents key in said field shown by said access information.

[Claim 11] It is the authentication correspondence procedure used in digital information from the record medium which has the field which memorizes digital information, and said field with the authentication communication system which consists of access equipment which writes digital information in read-out or said field. By transmitting the disturbance-ized access information which disturbed and generated the access information which shows said field from said access equipment to said record medium The 1st authentication step with which said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication step with which said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment The authentication correspondence procedure characterized by including the transfer step which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.

[Claim 12] Said field to the record medium which has the field which memorizes digital information, and digital information are constituted from access equipment which writes digital information in read-out or said field. After attesting justification of each device between said record media and said access equipment It is the record medium which is recording the authentication communications program used with the authentication communication system which transmits digital information and in which computer reading is possible. Said authentication communications program By transmitting the disturbance-ized access information which disturbed and generated the access information which shows said field from said access equipment to said record medium The 1st authentication step with which said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication step with which said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment The record medium characterized by including the transfer step which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.

[Claim 13] Access equipment which constitutes authentication communication system according to claim 1.

[Claim 14] Access equipment which constitutes authentication communication system according to claim 2.

[Claim 15] The record medium which constitutes authentication communication

system according to claim 1.
[Claim 16] The record medium which constitutes authentication communication system according to claim 3.
[Claim 17] Said field to the record medium which has the field which memorizes digital information, and digital information are constituted from access equipment which writes digital information in read-out or said field. After attesting justification of each device between said record media and said access equipment By transmitting the disturbance-ized access information which is the authentication communications program used with the authentication communication system which transmits digital information, and disturbed and generated the access information which shows said field to said record medium from said access equipment The 1st authentication step with which said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication step with which said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment The authentication communications program characterized by including the transfer step which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the technique which attests justification mutually between a device and a record medium, when transmitting a digital work between a device and a record medium.
[0002]
[Description of the Prior Art] Distributing them to each home through a communication line in recent years by the explosive spread of progress of digital information compression technology and the global telecom infrastructures represented by the Internet, using works, such as music, an image, an image, and a game, as a digital work is realized.
[0003] In order to establish the negotiation distribution system for protecting the access of the copyright person of a digital work, and a negotiation contractor's profit Unjust acquisition of the work by communicative wire tapping, tapping, spoofing, etc.,

and the illegal duplicate from the record medium which is recording the received data, It has been a technical problem to prevent malfeasances, such as an illegal alteration, it distinguishes that it is the system of normal, or work protection techniques, such as a code which performs a data scramble, and authentication, are needed.
[0004] More various things than before are known about the work protection technique, and in case the secret data storage area where the secret data which require protection of a work are stored as a typical thing is accessed, exchange of a random number and a response value is performed between devices, justification is attested mutually, it is suited, and only when just, there is a mutual recognition technique of the challenge response mold which permits access.
[0005]
[Problem(s) to be Solved by the Invention] However, for example, after performing mutual recognition using a regular device, the act which receives secret data unjustly can be considered by becoming a just device, clearing up and accessing a secret data storage area. Then, this invention is made in view of this trouble, and it aims at offering the record medium and authentication communications program which are recording the access equipment with which the information for accessing a secret data storage area is not revealed, a record medium, authentication communication system, the authentication correspondence procedure, and the authentication communications program.
[0006]
[Means for Solving the Problem] The record medium which has the field where this invention memorizes digital information in order to attain the above-mentioned object, It is the authentication communication system which consists of access equipment which writes digital information in digital information read-out or said field from said field. By transmitting the disturbance-ized access information which disturbed and generated the access information which shows said field from said access equipment to said record medium The 1st authentication phase when said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication phase when said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment It is characterized by including the transfer phase which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.
[0007] It sets here at said 1st authentication phase. Said access equipment The access information acquisition section which acquires the access information which shows said field, and the random-number acquisition section which acquires a random number, The generation section which compounds said acquired access information

and the acquired random number, and generates random-number-ized access information, The cryptopart which gives cryptographic algorithm to the generated random-number-ized access information, and generates disturbance-ized access information is included. Said record medium Including the response value generation section which generates a response value from the generated disturbance-ized access information, using said generated response value, said access equipment may be constituted so that the authentication section which attests justification of said record medium may be included.

[0008] Here, in said transfer phase, said record medium may be constituted so that the decode section which gives a decode algorithm to the generated disturbance-ized access information, and generates random-number-ized access information, and the separation section which separates access information from the transmitted random-number-ized access information may be included. Here, in said 1st authentication phase, including the random-number kind storage section said access equipment has remembered the random-number kind to be further, by reading a random-number kind from the random-number kind storage section, said random-number acquisition section may be constituted so that a random number may be acquired.

[0009] Here, in said 1st authentication phase, said access equipment may be constituted so that said random-number kind storage section may be further overwritten by using said disturbance-ized access information as a random-number kind. Here, in said 1st authentication phase, including the random-number kind storage section said access equipment has remembered the random-number kind to be further, by generating a random number based on the random-number kind which read and read the random-number kind from the random-number kind storage section, said random-number acquisition section may be constituted so that a random number may be acquired.

[0010] Here, in said 1st authentication phase, said access equipment may be constituted so that said random-number kind storage section may be further overwritten by using said generated random number as a random-number kind. In said transfer phase, the record medium which is recording digital information on said field here Digital information is read from said field shown by said access information. Said access equipment which reads digital information from said field including the cryptopart which gives cryptographic algorithm to the read digital information and generates encryption digital information Including the decode section which gives a decode algorithm to the generated encryption digital information, and generates DESHITARU information, said decode algorithm may be constituted so that the cipher generated by said cryptographic algorithm may be decoded.

[0011] In said transfer phase, said access equipment which writes digital information in said field here The digital information acquisition section which acquires digital information, and the cryptopart which gives cryptographic algorithm to the acquired digital information and generates encryption DESHITARU information are included.

Said record medium Give a decode algorithm to said generated encryption digital information, and digital information is generated. Including the decode section which writes digital information in said field shown by said access information, said decode algorithm may be constituted so that the cipher generated by said cryptographic algorithm may be decoded.

[0012] In said transfer phase, said access equipment which writes digital information in said field here The digital information acquisition section which acquires digital information, and the contents key acquisition section which acquires a contents key, The 1st cryptopart which gives the 1st cryptographic algorithm to the acquired contents key, and generates an encryption contents key, The 2nd encryption section which gives the 2nd cryptographic algorithm to said generated encryption contents key, and generates a duplex encryption contents key, The 3rd cryptopart which gives the 2nd cryptographic algorithm to said acquired digital information using said contents key, and generates encryption DESHITARU information is included. Said record medium Give the 1st decode algorithm to said generated duplex encryption contents key, and an encryption contents key is generated. Including the decode section which writes an encryption contents key in said field shown by said access information, said record medium may be constituted so that the field which memorizes said generated encryption digital information further may be included.

[0013]

[Embodiment of the Invention] The authentication communication system 100 as a gestalt of one operation concerning this invention is explained.

1. The appearance of the authentication communication system 100 and the external view of the authentication communication system 30 and 31 as a concrete example of a configuration of the utilization gestalt authentication communication system 100 are shown in drawing 1 (a) and (b).

[0014] As shown in drawing 1 (a), the authentication communication system 30 consists of a personal computer and a memory card 20. The personal computer is equipped with the display section, a keyboard, the loudspeaker, the microprocessor, RAM and ROM, the hard disk unit, etc., and is connected to the network represented by the Internet via a communication line. A memory card 20 is inserted from memory card insertion opening, and a personal computer is equipped with it.

[0015] As shown in drawing 1 (b), the authentication communication system 31 consists of a headphone stereo cassette tape recorder, a memory card 20, and headphone. A memory card 20 is inserted from memory card insertion opening of a headphone stereo cassette tape recorder, and a headphone stereo cassette tape recorder is equipped with it. The manual operation button of plurality [headphone stereo cassette tape recorder / top face] is arranged, and headphone are connected at another side face.

[0016] A user equips a personal computer with a memory card 20, and writes the digital work which incorporated and incorporated digital works, such as music, in a

memory card 20 from external Web server equipment via the Internet. Next, a user equips a headphone stereo cassette tape recorder with the memory card 20 on which the digital work is recorded, and it reproduces with a headphone stereo cassette tape recorder, and he enjoys the digital work currently recorded on the memory card 20.
[0017] Only when it is attested here that justification of each device by the Challenge Handshake Authentication Protocol of a challenge response mold is attested in between a headphone stereo cassette tape recorder and memory cards 20 in between a personal computer and memory cards 20, and it is a device just to mutual, a transfer of a digital work is performed between each device.
2. The configuration authentication communication system 100 of the authentication communication system 100 consists of reader writer equipment 10 and a memory card 20, as shown in drawing 2 . Here, reader writer equipment 10 is equivalent to the personal computer and headphone stereo cassette tape recorder which are shown in drawing 1 (a) and (b).
[0018] 2.1 The configuration reader writer equipment 10 of reader writer equipment 10 consists of the **** generation section 108, the code decode section 109, the data storage section 110, and the I/O section 111 at the access information storage section 101, the random-number kind storage section 102, the synthetic section 103, the common key storage section 104, the encryption section 105, the renewal section 106 of a random-number kind, the mutual recognition section 107, and the time.
[0019] As for reader writer equipment 10, it specifically has a microprocessor, RAM, and ROM and others, the computer program is recorded on ROM etc., and a microprocessor operates according to said computer program.
(1) The I/O section 111 I/O section 111 receives actuation of a user, and generates the access information for accessing the music information memorized by the data storage section 209 of a memory card 20. As shown in drawing 3 , access information is 32 bit length and consists of address information which shows the address of the field of the data storage section of a memory card 20, and size information which shows the size of said field. Address information is 24 bit length and size information is 8 bit length.
[0020] Moreover, from the data storage section 110, the I/O section 111 reads the music information CT, and changes and outputs the read music information CT to a sound signal. Moreover, the I/O section 111 receives actuation of a user and writes from the exterior the music information CT which acquired and acquired the music information CT in the data storage section 110.
(2) The access information storage section 101 access-information storage section 101 consisted of semiconductor memory, and, specifically, is equipped with the field which memorizes access information.
[0021] (3) The random-number kind storage section 102 random-number kind storage section 102 consisted of semiconductor memory, and, specifically, has memorized beforehand the random-number kind of 64 bit length as shown in drawing 3 . A

random-number kind is recorded at the time of manufacture of equipment. The random-number kind storage section 102 does not have the means which can carry out direct access from the outside, but is a storage means protected.
[0022] (4) The synthetic section 103 composition section 103 reads access information from the access information storage section 101, and reads a random-number kind from the random-number kind storage section 102. next, as shown in drawing 3 , 32 bits of said random-number kind which carried out reading appearance to said access information which carried out reading appearance of low order are combined, and the random-number-ized access information of 64 bit length is generated. The generated random-number-ized access information is outputted to the encryption section 105.
[0023] (5) The common key storage section 104 common key storage section 104 consisted of semiconductor memory, and, specifically, is equipped with the field which memorizes the common key UK of 56 bit length. Reader writer equipment 10 acquires in secrecy the common key UK memorized by the common key storage section 201 from a memory card 20, and the common key storage section 104 memorizes the acquired common key UK.
[0024] The common key storage section 104 does not have the means which can carry out direct access from the outside, but is a storage means protected.
(6) The encryption section 105 encryption section 105 reads the common key UK from the common key storage section 104, and receives random-number-ized access information from the synthetic section 103. Next, the encryption section 105 gives cryptographic algorithm E1 to the received random-number-ized access information using the common key UK, and generates the encryption access information R1. Here, DES (Data Encryption Standard) is used for the encryption section 105 as cryptographic algorithm E1.
[0025] Next, the encryption section 105 outputs the generated encryption access information R1 to the **** generation section 108 at the time with the mutual recognition section 107 and the renewal section 106 of a random-number kind. Moreover, the generated encryption access information R1 is outputted to the **** generation section 208 at the time with the decryption section 205 of a memory card 20, and the mutual recognition section 207. Thus, the generated encryption access information R1 is disturbance-ized information acquired by performing disturbance (scramble) processing to access information.
[0026] (7) It uses received encryption access information R1 as a new random-number kind by using encryption access information R1 as reception from the encryption section 105, and the renewal section 106 of a renewal section of random-number kind 106 random-number kind overwrites it to the random-number kind storage section 102.
(8) The mutual recognition section 107 mutual-recognition section 107 computes response value V2' by the formula 1 using R1 and the common key UK which read the

encryption access information R1 and received reception and the common key storage section 104 to the common key UK.
(Formula 1) V2'=F1(R1, UK) =SHA (R1+UK)
Here, a function F1 (a, b) is a function which combines a and b and gives SHA (Secure Hash Algorithm) to the joint result as an example. In addition, + is a operator which shows association.
[0027] The mutual recognition section 107 receives the response value V2 from the mutual recognition section 207. Next, it judges whether V2 and V2' of the mutual recognition section 107 corresponds, and in not being in agreement, it presumes that a memory card 20 is inaccurate equipment, and forbids [subsequent] activation of operation to other configuration sections. In being in agreement, the mutual recognition section 107 presumes that a memory card 20 is just equipment, and it permits [subsequent] activation of operation to other configuration sections.
[0028] Moreover, the mutual recognition section 107 outputs the response value V1 which computed the response value V1 and computed the random number R2 by the formula 2 using reception, the received random number R2, and said common key UK from the random-number generation section 204 to the mutual recognition section 207.
(Formula 2) V1=F2(R2, UK) =SHA (R2+UK)
(9) the time -- **** -- generation -- the section -- 108 -- o'clock -- **** -- generation -- the section -- 108 -- a memory card -- 20 -- being just -- equipment -- it is -- ** -- recognizing -- having -- the case of actuation where activation is permitted -- the encryption access information R1 and a random number R2 -- reception, and R1 and R2 to the formula 3 -- using -- the time -- **** VK -- generating -- (formula 3) VK=F3(R1, R2) =SHA (R1+R2)
next, the time -- the **** generation section 108 -- having generated -- the time -- **** VK -- the code decode section 109 -- outputting .
[0029] (10) the code decode section 109 code decode section 109 -- the time -- the time from the **** generation section 108 -- **** VK -- receiving . The code decode section 109 gives [from the code decode section 210] the decode algorithm D3 to the encryption music information EncCT using **** VK at reception and said time for the encryption music information EncCT, and writes the music information CT which generated and generated the music information CT in the data storage section 110.
[0030] Here, DES is used for the code decode section 109 as a decode algorithm E3. Moreover, the code decode section 109 reads the music information CT from the data storage section 110, gives cryptographic algorithm E2 to the music information CT using **** VK at said time, and outputs the encryption music information EncCT which generated and generated the encryption music information EncCT to the code decode section 210.
[0031] Here, DES is used for the code decode section 109 as cryptographic algorithm

E2.
(11) The data storage section 110 data-storage section 110 consisted of semiconductor memory, and, specifically, is equipped with the field which memorizes the music information CT.
[0032] 2.2 Memory card 20 memory card 20 consists of the **** generation section 208, the data storage section 209, and the code decode section 210 at the common key storage section 201, the random-number kind storage section 202, the renewal section 203 of a random-number kind, the random-number generation section 204, the decryption section 205, the separation section 206, the mutual recognition section 207, and the time.
[0033] (1) The common key storage section 201 common key storage section 201 consisted of semiconductor memory, and, specifically, has memorized the common key UK of 56 bit length. The common key UK is recorded at the time of manufacture of a memory card 20. The common key storage section 201 does not have the means which can carry out direct access from the outside, but is a storage means protected.
[0034] (2) The random-number kind storage section 202 random-number kind storage section 202 consisted of semiconductor memory, and, specifically, has memorized the random-number kind of 64 bit length beforehand. A random-number kind is recorded at the time of manufacture of a memory card 20. The random-number kind storage section 202 does not have the means which can carry out direct access from the outside, but is a storage means protected.
[0035] (3) The random-number generation section 204 random-number generation section 204 Read, generate and the random number R2 which generated the random number R2 of 64 bit length using the random-number kind which read the random-number kind from the random-number kind storage section 202 The renewal section 203 of a random-number kind, The mutual recognition section 207 and the random number R2 which outputted to the **** generation section 208 at the time, and was generated are outputted to the **** generation section 108 with the mutual recognition section 107 of reader writer equipment 10 at the time.
[0036] (4) It uses the received random number R2 as a new random-number kind by using a random number R2 as reception from the random-number generation section 204, and the renewal section 203 of a renewal section of random-number kind 203 random-number kind overwrites it to the random-number kind storage section 202.
(5) The decryption section 205 decryption section 205 reads the common key UK from the common key storage section 201, and receives the encryption access information R1 from the encryption section 105. Next, using the read common key UK, the decode algorithm D1 is given to the received encryption access information R1, and the random-number-ized access information which generated and generated random-number-ized access information is outputted to it to the separation section 206.
[0037] Here, DES is used for the decryption section 205 as a decode algorithm D1.

The decode algorithm D1 decodes the cipher generated by cryptographic algorithm E1.
(6) The separation section 206 separation section 206 separates data of 32 bits of reception and the received random-number-ized access information to the high order for random-number-ized access information from the decryption section 205 as access information, and outputs access information to the data storage section 209.
[0038] (7) The mutual recognition section 207 mutual-recognition section 207 reads the common key UK from the common key storage section 201, and outputs V2 which computed the response value V2 and computed the encryption access information R1 by the formula 4 using reception, and R1 and the common key UK which were received to the mutual recognition section 107 of reader writer equipment 10.
(Formula 4) V2=F1(R1, UK) =SHA (R1+UK)
Here, F1 should just be the same function as F1 shown in a formula 1.
[0039] Moreover, the mutual recognition section 207 computes response value V1' for a random number R2 by the formula 5 using reception, the received random number R2, and said common key UK from the random-number generation section 204.
(Formula 5) V1'=F2(R2, UK) =SHA (R2+UK)
Here, F2 should just be the same function as F2 shown in a formula 2.
[0040] Next, the mutual recognition section 207 judges whether reception, and V1 and V1' are in agreement in V1 from the mutual recognition section 107, and in not being in agreement, it presumes that reader writer equipment 10 is inaccurate equipment, and forbids [subsequent] activation of operation to other configuration sections. In being in agreement, the mutual recognition section 207 presumes that reader writer equipment 10 is just equipment, and it permits [subsequent] activation of operation to other configuration sections.
[0041] (8) the time -- **** -- generation -- the section -- 208 -- o'clock -- **** -- generation -- the section -- 208 -- a reader -- a writer -- equipment -- ten -- being just -- equipment -- it is -- ** -- recognizing -- having -- the case of actuation where activation is permitted -- the encryption access information R1 and a random number R2 -- reception, and R1 and R2 to the formula 6 -- using -- the time -- **** VK -- generating -- (formula 6) VK=F3(R1, R2) =SHA (R1+R2)
Here, F3 is the same as the function F3 shown in a formula 3.
[0042] next, the time -- the **** generation section 208 -- having generated -- the time -- **** VK -- the code decode section 210 -- outputting .
(9) The data storage section 209 data-storage section 209 consisted of semiconductor memory, and, specifically, is equipped with the field which memorizes the music information CT.
[0043] (10) the code decode section 210 code decode section 210 -- the time -- the time from the **** generation section 208 -- **** VK -- receiving . The code decode section 210 gives [from the code decode section 109] the decode algorithm D2 to the encryption music information EncCT using **** VK at reception and said time for the encryption music information EncCT, and writes the music information

CT which generated and generated the music information CT in the field shown by said access information of the data storage section 209.
[0044] Here, DES is used for the code decode section 210 as a decode algorithm D2. The decode algorithm D2 decodes the cipher generated by cryptographic algorithm E2. Moreover, the code decode section 210 reads the music information CT from the field shown by said access information of the data storage section 209, gives cryptographic algorithm E3 to the music information CT using **** VK at said time, and outputs the encryption music information EncCT which generated and generated the encryption music information EncCT to the code decode section 109.
[0045] Here, DES is used for the code decode section 210 as cryptographic algorithm E3. The decode algorithm D3 decodes the cipher generated by cryptographic algorithm E3.
3. Explain actuation of the reader writer equipment 10 and the memory card 20 which constitute of operation (1) read-out actuation authentication communication system 100 of the authentication communication system 100 using the flow chart shown in drawing 4 - drawing 5 .
[0046] In addition, it assumes that reader writer equipment 10 is equipment which reads the information memorized by the memory card like the headphone stereo cassette tape recorder shown in drawing 1 (b), and explains here. The synthetic section 103 carries out reading appearance of the random-number kind from the random-number kind storage section 102, and said access information which carried out reading appearance to said random-number kind which carried out reading appearance of the access information, and carried out reading appearance is compounded from the access information storage section 101. Random-number-ized access information is generated (step S101). The encryption section Encipher random-number-ized access information using said common key which read the common key and was read from the common key storage section 104, and the encryption access information R1 is generated (step S102). The mutual recognition section 107 computes V2'=F1 (R1) (step S103), and the renewal section 106 of a random-number kind uses generated random-number-ized access information as a new random-number kind, and it overwrites the random-number kind storage section 102 (step S104).
[0047] The encryption section 105 outputs the generated encryption access information R1 to a memory card 20, and the mutual recognition section 207 of a memory card receives the encryption access information R1 (step S105). The mutual recognition section 207 computes V2=F1 (R1) (step S106), V2 is outputted to the mutual recognition section 107 of reader writer equipment 10, and the mutual recognition section 107 receives V2 (step S107).
[0048] It judges whether V2 and V2' of the mutual recognition section 107 corresponds, and in not being in agreement, (step S108) and a memory card 20 presume that it is inaccurate equipment, and stop future actuation. In being in

agreement, (step S108) and the mutual recognition section 107 It presumes that a memory card 20 is just equipment. The random-number generation section 204 of a memory card 20 From the random-number kind storage section 202, a random-number kind is read and a random number R2 is generated using the read random-number kind (step S109). The mutual recognition section 207 V1'=F2 (R2) is computed (step S110), and the renewal section 203 of a random-number kind newly overwrites the random-number kind storage section 202 by using the generated random number R2 as a random-number kind (step S111). Next, the random-number generation section 204 outputs the generated random number R2 to the mutual recognition section 107 of reader writer equipment 10, the mutual recognition section 107 generates a random number R2, reception (step S112) and the mutual recognition section 107 generate V1=F2 (R2) (step S113), V1 generated is outputted to the mutual recognition section 207 of a memory card 20, and the mutual recognition section 207 receives V1 (step S114).

[0049] Next, it judges whether V1 and V1' of the mutual recognition section 207 mutual-recognition section 207 corresponds, and in not being in agreement, (step S115) and reader writer equipment 10 presume that it is inaccurate equipment, and stop future actuation. the time of (step S115) and the mutual recognition section 207 presuming that reader writer equipment 10 is just equipment, in being in agreement, and being reader writer equipment 10 -- the **** generation section 108 -- R1 and R2 -- using -- the time -- **** VK -- generating (step S121) . The decryption section 205 of a memory card 20 reads the common key UK from the common key storage section 201. R1 is decoded using the read common key UK, and random-number-ized access information is generated (step S122). The separation section 206 random-number-ized access information to access information -- dissociating (step S123) -- the time -- the **** generation section 208 -- R1 and R2 -- using -- the time -- **** VK -- generating (step S124) -- the code decode section 210 -- The music information CT is read from the field of the data storage section 209 shown by access information (step S125). The code decode section 210 When generated, said music information CT read using **** VK is enciphered, and the encryption music information EncCT which generated and (step S126) generated the encryption music information EncCT is outputted to the code decode section 109 of reader writer equipment 10 (step S127).

[0050] the code decode section 109 -- the time -- **** VK -- using -- the encryption music information EncCT -- decoding -- the music information CT -- generating -- the data storage section 110 -- writing in (step S128) -- the I/O section 111 -- the music information CT -- the reading appearance from the data storage section 110 -- it carries out, and the music information CT which carried out reading appearance is changed and outputted to a sound signal (step S129).

(2) Explain actuation of the reader writer equipment 10 and the memory card 20 which constitute the write-in actuation authentication communication system 100

using the flow chart shown in drawing 6 .
[0051] Here, like the personal computer shown in drawing 1 (a), reader writer equipment 10 assumes that it is equipment which writes in information to a memory card, and explains to it. Moreover, since read-out actuation and write-in actuation are similar, only a point of difference is explained. If it transposes to the step which shows steps S125-S129 of the flow chart of drawing 4 - drawing 5 to drawing 6 , it will become write-in actuation of the authentication communication system 100.
[0052] a code -- decode -- the section -- 109 -- data storage -- the section -- 110 -- from -- music -- information -- CT -- reading -- appearance -- carrying out (step S131) -- the time -- **** -- VK -- using -- reading -- appearance -- having carried out -- music -- information -- CT -- enciphering -- encryption -- music -- information -- CT -- generating (step S132) -- having generated -- encryption -- music -- information -- CT -- the code decode section 210 of a memory card 20 -- outputting -- the code decode section 210 -- encryption music information CT -- receiving (step S133) .
[0053] a code -- decode -- the section -- 210 -- encryption -- music -- information -- EncCT -- the time -- **** -- VK -- using -- decoding -- music -- information -- CT -- generating (step S134) -- having generated -- music -- information -- CT -- said access information -- being shown -- having -- data storage -- the section -- 209 -- inside -- it writes in a field (step S135).
4. Since the information for accessing the secret data storage area which is recording secret data is disturbed and transmitted to mutual recognition and coincidence as explained more than the conclusion, the confidentiality of the information for accessing a secret data storage area can be raised.
[0054] Moreover, since mutual recognition is not established even if it is the case where the information for accessing a secret data storage area temporarily is altered and transmitted to another information by inaccurate spoofing, it can avoid accessing a secret data storage area. Moreover, since the access information for accessing a secret data storage area does not relate to renewal of a random number, the periodicity of a random number can be raised.
[0055] 5. Explain authentication communication system 100a as a modification of the authentication communication system 100a authentication communication system 100.
5.1 Configuration authentication communication system 100of authentication communication system 100a a consists of reader writer equipment 10a and a memory card 20, as shown in drawing 7 .
[0056] Since the memory card 20 is the same as the memory card 20 shown in drawing 2 , explanation is omitted here. Reader writer equipment 10a consists of the **** generation section 108, the code decode section 109, the data storage section 110, the I/O section 111, and the random-number generation section 112 at the access information storage section 101, the random-number kind storage section 102, the synthetic section 103, the common key storage section 104, the encryption

section 105, the renewal section 106 of a random-number kind, the mutual recognition section 107, and the time.
[0057] It explains below focusing on a point of difference with reader writer equipment 10. Since it is the same as reader writer equipment 10 about other points, explanation is omitted.
(1) From the random-number kind storage section 102, the random-number generation section 112 random-number generation section 112 reads a random-number kind, and outputs the random number which generated and generated the random number of 64 bit length using the read random-number kind to the synthetic section 103 and the renewal section 106 of a random-number kind.
[0058] (2) It uses the received random number as a new random-number kind by using a random number as reception from the random-number generation section 112, and the renewal section 106 of a renewal section of random-number kind 106 random-number kind overwrites it to the random-number kind storage section 102.
(3) the synthetic section 103 composition section 103 compounds said access information which carried out reading appearance to said random number which carried out reading appearance of reception and the access information storage section 101 to the access information for the random number, and was received from the random-number generation section 112, and generates random-number-ized access information.
[0059] 5.2 Explain actuation of of operation authentication communication system 100a of authentication communication system 100a using the flow chart shown in drawing 8 . the random-number generation section 112 generates the random number of 64 bit length using the random-number kind which carried out reading appearance of the random-number kind (step S201), and carried out reading appearance from the random-number kind storage section 102 (step S202), and it uses the received random number as a new random-number kind by using a random number as reception from the random-number generation section 112, and it overwrites the renewal section 106 of a random-number kind to the random-number kind storage section 102 (step S203). next, the synthetic section 103 compounds said access information which carried out reading appearance to said random number which carried out reading appearance of reception and the access information storage section 101 to the access information for the random number, and was received from the random-number generation section 112, and generates random-number-ized access information (step S204).
[0060] Next, it continues to step S102 of drawing 4 . Since the following is the same as actuation of the authentication communication system 100, explanation is omitted.
5.3 Since the access information for accessing a secret data storage area does not relate to renewal of a random number as explained more than the conclusion, the periodicity of a random number can be raised.
[0061] 6. Explain authentication communication system 100b as a modification of

authentication communication system 100b authentication communication system 100a.
6.1 Configuration authentication communication system 100of authentication communication system 100b b consists of reader writer equipment 10b and memory card 20b, as shown in drawing 9 .
[0062] (1) Configuration reader writer equipment 10of reader writer equipment 10b b At the access information storage section 101, the random-number kind storage section 102, the synthetic section 103, the common key storage section 104, the encryption section 105, the renewal section 106 of a random-number kind, the mutual recognition section 107, and the time, the **** generation section 108, the data storage section 110, the I/O section 111, the random-number generation section 112, the contents key generation section 113, It consists of the encryption section 114, the contents additional information storage section 115, the code decode section 116, and the encryption section 117.
[0063] A point of difference with reader writer equipment 10a is explained as a core below. Since it is the same as reader writer equipment 10a about other points, explanation is omitted.
(a) The I/O section 111 I/O section 111 receives the input of contents additional information by actuation of a user, and writes the received contents additional information in the contents additional information storage section 115.
[0064] Here, examples of contents additional information are the count of playback of contents, and duration of service, and contents additional information is 8 bit length. Moreover, the I/O section 111 acquires the contents data CD by actuation of a user, and writes the acquired contents data CD in the data storage section 110. Here, the contents data CD are music content information as an example.
[0065] (b) The random-number generation section 112 random-number generation section 112 outputs the generated random number R3 to the contents key generation section 113.
(c) the contents key generation section 113 contents key generation section 113 generates the contents key CK by the formula 7 using the contents additional information which carried out reading appearance of the contents additional information from the contents additional information storage section 115, and carried out reading appearance of the random number R3 to reception and a random number R3 from the random-number generation section 112. Here, the contents keys CK are 64 bit length.
(Formula 7) CK=F4 (R3, contents additional information)
= + is a operator which shows association of data and data here 56 bits of low order of contents additional information (8 bit length) +R3.
[0066] Next, the contents key generation section 113 outputs the generated contents key CK to the encryption section 114 and the encryption section 117.
(d) the encryption section 114 encryption section 114 gives encryption algorithm E4

to the contents key CK which received the contents key CK from the contents key generation section 113 using the common key UK which carried out reading appearance of the common key UK, and carried out reading appearance from reception and the common key storage section 104, and outputs the encryption contents key EncCK which generated and generated the encryption contents key EncCK to the code decode section 116.

[0067] Here, DES is used for the encryption section 114 as cryptographic algorithm E4.

(e) the code decode section 116 code decode section 116 -- the encryption section 114 to the encryption contents key EncCK -- reception and the received encryption contents key EncCK -- the time -- **** VK -- using -- cryptographic algorithm E -- give 2 and output Enc (EncCK) which generated and generated Enc (EncCK) to the code decode section 211.

[0068] Here, DES is used for the code decode section 116 as cryptographic algorithm E2.

(f) The encryption section 117 encryption section 117 uses the contents key CK for the contents data CD which read the contents data CD and were read from the data storage section 110, gives encryption algorithm E5, and generates the encryption contents data EncCD. Next, the encryption section 117 outputs the generated encryption contents data EncCD to the data storage section 213.

[0069] Here, DES is used for the encryption section 117 as cryptographic algorithm E5.

(2) Configuration memory card 20of memory card 20b b consists of the **** generation section 208, the code decode section 211, the key data storage section 212, and the data storage section 213 at the common key storage section 201, the random-number kind storage section 202, the renewal section 203 of a random-number kind, the random-number generation section 204, the decryption section 205, the separation section 206, the mutual recognition section 207, and the time.

[0070] A point of difference with a memory card 20 is explained as a core below. Since it is the same as a memory card 20 about other points, explanation is omitted.

(a) the time -- the **** generation section 208:00 **** generation section 208 -- the time -- **** VK -- the code decode section 211 -- outputting .

(b) the code decode section 211 code decode section 211 -- the time -- the time from the **** generation section 208 -- **** VK -- reception and the code decode section 116 to Enc (EncCK) -- receiving .

[0071] next -- a code -- decode -- the section -- 211 -- the time -- **** -- VK -- using -- Enc (EncCK) -- decode -- an algorithm -- D -- two -- giving -- encryption -- contents -- a key -- EncCK -- generating -- having generated -- encryption -- contents -- a key -- EncCK -- said -- access information -- being shown -- having -- a key -- data storage -- the section -- 212 -- it writes in a field.

(c) The key data storage section 212 key data storage section 212 is equipped with

the field which memorizes the encryption contents key EncCK.
[0072] (d) The data storage section 213 data-storage section 213 memorizes reception and the received encryption contents data EncCD for the encryption contents data EncCD.
6.2 Actuation of of operation authentication communication system 100b of authentication communication system 100b is similar to actuation of authentication communication system 100a. Here, only a point of difference with authentication communication system 100a is explained.
[0073] Actuation of authentication communication system 100b is shown by the flow chart replaced with the flow chart which shows step S121 or subsequent ones to drawing 10 among the flow charts which show actuation of authentication communication system 100a. The contents key generation section 113 reads contents additional information from the contents additional information storage section 115 (step S301). The random-number generation section 112 The generated random number R3 is outputted to the contents key generation section 113. The contents key generation section 113 Using the contents additional information which read R3 with reception and R3, generate and the contents key CK which generated the contents key CK from the random-number generation section 112 The encryption section 114, It outputs to the encryption section 117 (step S302). The encryption section 114 Reception and the common key storage section 104 to the common key UK is read for the contents key CK from the contents key generation section 113. Encryption algorithm E4 is given to the received contents key CK using the read common key UK, and the encryption contents key EncCK which generated and generated the encryption contents key EncCK is outputted to the code decode section 116 (step S303). The code decode section 116 the encryption contents key EncCK Next, reception, 2 is given and Enc (EncCK) is generated (step S304). the received encryption contents key EncCK -- the time -- **** VK -- using -- cryptographic algorithm E -- the code decode section 116 Generated Enc (EncCK) is outputted to the code decode section 211. The code decode section 211 Enc (EncCK) reception (step S305) and the code decode section 211 Enc (EncCK) -- the time -- **** -- VK -- using -- decode -- an algorithm -- D -- two -- giving -- encryption -- contents -- a key -- EncCK -- generating -- having generated -- encryption -- contents -- a key -- EncCK -- said access information -- being shown -- having -- a key -- data storage -- the section -- 212 -- it writes in a field (step S306).
[0074] the encryption section 117 uses the contents key CK for the contents data CD which carried out reading appearance of the contents data CD (step S307), and carried out reading appearance from the data storage section 110, gives encryption algorithm E5, and generates the encryption contents data EncCD (step S308). The encryption section 117 outputs the generated encryption contents data EncCD to the data storage section 213, and the data storage section 213 memorizes the encryption contents data EncCD with which reception (step S309) and the data storage section

213 received the encryption contents data EncCD (step S310).
[0075] 6.3 As explained more than the conclusion, although the contents key for enciphering contents data is generated, in authentication communication system 100b,-izing of the new random-number-generation device can be carried out [****] with the need, and **** and the random-number-generation device in which it uses for composition of access information.
7. Although this invention has been explained based on the gestalt of the above-mentioned operation, this invention of not being limited [which are other modifications] to the gestalt of the above-mentioned operation is natural. It is contained in this invention also when as follows.
[0076] (1) the gestalt of the above-mentioned operation -- setting -- a digital work -- a sound -- although it is easy information, it is good though it is dynamic images, such as static images, such as compressed voice data which is represented by alphabetic data, such as a novel and a paper, the computer program software for computer games, MP3, etc., and JPEG, and MPEG. Moreover, though reader writer equipment is an output unit which is not limited to a personal computer, but sells or distributes the above-mentioned various digital works, it is good. Moreover, though reader writer equipment is a regenerative apparatus which is not limited to a headphone stereo cassette tape recorder, but reproduces a digital work, it is good. For example, it is good though it is computer-game equipment, a band type information terminal, a dedicated device, a personal computer, etc. Moreover, though reader writer equipment combines both the above-mentioned output unit and the regenerative apparatus, it is good.
[0077] (2) In the gestalt of the above-mentioned operation, although [an algorithm] DES is used, though other codes are used for cryptographic algorithm and a decode algorithm, they are good. Moreover, in the gestalt of the above-mentioned implementation, although SHA is used, though other one direction nature functions are used, it is good. At a common key and the time, although [length] it is 56 bits, though the key of other die length is used for the key length of ****, it is good.
[0078] (3) In the gestalt of the above-mentioned operation, the synthetic section 103 combines 32 bits of low order of a random-number kind with access information, and although [the section] the random-number-ized access information of 64 bit length is generated, it is not limited to this. You may make it be a degree. The synthetic section 103 combines 32 bits of 1 bit of low order of a random-number kind with 32-bit access information at a time by turns, generates the random-number-ized access information of 64 bit length, and its potato is good. Moreover, two or more bits may combine at a time by turns. In this case, the separation section 206 is made to operate reverse.
[0079] (4) In the gestalt of the above-mentioned operation, although [the random-number generation section 204 of a memory card 20] a random number R2 is generated using the random-number kind memorized by the random-number kind

storage section 202, the random-number generation section 204 may generate a random-number kind as a random number R2. moreover, the time -- the **** generation sections 108 and 208 -- R1 and R2 -- using -- the time -- **** -- generating -- ** -- carrying out -- **** -- although -- a response value -- using -- ****** -- being good . Moreover, the common key UK may be twined.

[0080] (5) In authentication communication system 100b, although the encryption contents data EncCD are written in the data storage section 213, though the encryption section 117 is written in the field which treats the encryption contents data EncCD as secret data, and is shown by access information, it is good. Moreover, it is good though the encryption contents key EncCK is written in the data storage section 213, without treating as secret data.

[0081] Moreover, it loses, and it remains, while either the encryption section 114 and the encryption section 117 may be share-ized.

(6) Though this invention is an approach shown above, it is good. Moreover, though it is the computer program which realizes these approaches by computer, it is good, and it is good though it is the digital signal which consists of said computer program.

[0082] Moreover, this invention is good also as what recorded said computer program or said digital signal on the record medium in which computer reading is possible, for example, a floppy (trademark) disk, a hard disk, CD-ROM, MO and DVD, DVD-ROM, DVD-RAM, semiconductor memory, etc. Moreover, it is good though it is said computer program currently recorded on these record media, or said digital signal.

[0083] Moreover, this invention is good also as what is transmitted via the network where said computer program or said digital signal is used into a telecommunication circuit, wireless, or a wire communication circuit, and it uses the Internet representation. Moreover, this invention is the computer system equipped with a microprocessor and memory, said memory has memorized the above-mentioned computer program, and though said microprocessor operates according to said computer program, it is good.

[0084] moreover, the thing for which said program or said digital signal is recorded on said record medium, and is transported -- or by transporting said program or said digital signal via said network etc., though carried out according to other independent computer systems, it is good.

(4) It is good though the gestalt and the above-mentioned modification of the above-mentioned implementation are combined, respectively.

[0085] 8. When reproducing a digital work to a semi-conductor record medium from the output unit which outputs the possibility digital work of utilization on industry and an output unit and a semi-conductor record medium attest justification mutually, it can use. Moreover, when reading a digital work, reproducing from the semi-conductor record medium with which the digital work is recorded and each equipment attests justification mutually between a semi-conductor record medium and a regenerative apparatus, it can use.

[0086]
[Effect of the Invention] The record medium which has the field where this invention memorizes digital information in order to attain the above-mentioned object, It is the authentication communication system which consists of access equipment which writes digital information in read-out or said field in digital information from said field. By transmitting the disturbance-ized access information which disturbed and generated the access information which shows said field from said access equipment to said record medium The 1st authentication phase when said access equipment attests justification of said record medium by the Challenge Handshake Authentication Protocol of a challenge response mold, When both the 2nd authentication phase when said record medium attests justification of said access equipment, and said record medium and said access equipment are attested with having justification, said record medium Access information is extracted from the transmitted disturbance-ized access information. Said access equipment It is characterized by including the transfer phase which writes digital information in the field which reads digital information from the field shown by said extracted access information, or is shown by said access information.
[0087] Since the information for accessing the secret data storage area which is recording secret data is disturbed and transmitted to mutual recognition and coincidence by this, the confidentiality of the information for accessing a secret data storage area can be raised. Moreover, since mutual recognition is not successful temporarily even if the information for accessing a secret data storage area is the case where it is altered and transmitted to another information by inaccurate spoofing, it can avoid accessing a secret data storage area.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] Drawing 1 shows the appearance of the authentication communication system 30 and 31 as a concrete example of a configuration of the authentication communication system 100. Drawing 1 (a) shows the appearance of a personal computer and the authentication communication system 30 which consists of memory cards 20, and drawing 1 (b) shows the appearance of the authentication communication system 31 which consists of a headphone stereo cassette tape recorder, a memory card 20, and headphone.
[Drawing 2] Drawing 2 is the reader writer equipment 10 which constitutes the authentication communication system 100, and the block diagram of a memory card 20 showing a configuration, respectively.

[Drawing 3] Drawing 3 shows the DS of access information, random-number kind, and random-number-ized access information.
[Drawing 4] Drawing 4 is a flow chart which shows actuation of the authentication communication system 100, and assumes the case where the information especially memorized by the memory card is read. Drawing 5 is followed.
[Drawing 5] Drawing 5 is a flow chart which shows actuation of the authentication communication system 100. It continues from drawing 4 .
[Drawing 6] It is a thing at the time of assuming that drawing 6 is a flow chart which shows actuation of the authentication communication system 100, and especially reader writer equipment 10 is equipment which writes information in a memory card.
[Drawing 7] Drawing 7 is the block diagram showing the configuration of authentication communication system 100a as a gestalt of another operation.
[Drawing 8] Drawing 8 is a flow chart which shows actuation of a proper to authentication communication system 100a.
[Drawing 9] Drawing 9 is the block diagram showing the configuration of authentication communication system 100b as a gestalt of another operation.
[Drawing 10] Drawing 10 is a flow chart which shows actuation of a proper to authentication communication system 100b.
[Description of Notations]
100 Authentication Communication System
10 Reader Writer Equipment
101 Access Information Storage Section
102 Random-Number Kind Storage Section
103 Synthetic Section
104 Common Key Storage Section
105 Encryption Section
106 Renewal Section of Random-Number Kind
107 Mutual Recognition Section
108 the Time -- **** Generation Section
109 Code Decode Section
110 Data Storage Section
111 I/O Section
20 Memory Card
201 Common Key Storage Section
202 Random-Number Kind Storage Section
203 Renewal Section of Random-Number Kind
204 Random-Number Generation Section
205 Decryption Section
206 Separation Section
207 Mutual Recognition Section
208 the Time -- **** Generation Section

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－306401
（P2001－306401A）
(43)公開日　平成13年11月2日(2001.11.2)

(51)Int.Cl.'	識別記号	ＰＩ		ﾃｰﾏｺｰﾄﾞ'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
			３２０Ｂ	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ	５Ｂ０５８
19/07		Ｇ０９Ｃ　1/00	６６０Ｆ	５Ｊ１０４
19/10		Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数17　ＯＬ　（全 17 頁）　最終頁に続く

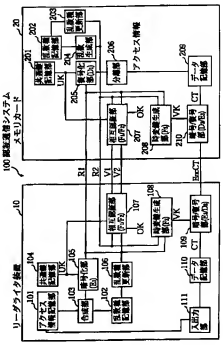
(21)出願番号　特願2001－4730(P2001－4730)
(22)出願日　平成13年１月12日(2001.1.12)
(31)優先権主張番号　特願2000－6989(P2000－6989)
(32)優先日　平成12年１月14日(2000.1.14)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2000－41317(P2000－41317)
(32)優先日　平成12年２月18日(2000.2.18)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　柴田　修
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　湯川　泰平
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　認証通信装置及び認証通信システム

(57)【要約】
【課題】　機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置を提供する。
【解決手段】　アクセス装置において、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を記録媒体へ伝送することにより、チャレンジレスポンス型の認証プロトコルによる記録媒体の正当性の認証を行う。記録媒体において、アクセス装置の正当性の認証を行う。記録媒体とアクセス装置とがともに正当性を有すると認証された場合に、記録媒体において、伝送された攪乱化アクセス情報からアクセス情報を分離し、アクセス装置において、分離された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む。



【特許請求の範囲】

【請求項１】　デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を撹乱して生成した撹乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証フェーズと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証フェーズと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された撹乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする認証通信システム。

【請求項２】　前記第１認証フェーズにおいて、

前記アクセス装置は、

前記領域を示すアクセス情報を取得するアクセス情報取得部と、

乱数を取得する乱数取得部と、

取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、

生成した乱数化アクセス情報に暗号アルゴリズムを施して撹乱化アクセス情報を生成する暗号部とを含み、

前記記録媒体は、

生成された撹乱化アクセス情報から応答値を生成する応答値生成部とを含み、

前記アクセス装置は、

生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う認証部を含むことを特徴とする請求項１に記載の認証通信システム。

【請求項３】　前記転送フェーズにおいて、

前記記録媒体は、

生成された撹乱化アクセス情報に復号アルゴリズムを施して乱数化アクセス情報を生成する復号部と、

伝送された乱数化アクセス情報からアクセス情報を分離する分離部とを含むことを特徴とする請求項２に記載の認証通信システム。

【請求項４】　前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、乱数を取得することを特徴とする請求項３に記載の認証通信システム。

【請求項５】　前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、

前記撹乱化アクセス情報を乱数種として前記乱数種記憶部に上書きすることを特徴とする請求項４に記載の認証通信システム。

【請求項６】　前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した乱数種に基づいて乱数を生成することにより、乱数を取得することを特徴とする請求項３に記載の認証通信システム。

【請求項７】　前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、

生成された前記乱数を乱数種として前記乱数種記憶部に上書きすることを特徴とする請求項６に記載の認証通信システム。

【請求項８】　前記転送フェーズにおいて、

前記領域にデジタル情報を記録している記録媒体は、

前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

前記領域からデジタル情報を読み出す前記アクセス装置は、

生成された暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成する復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号することを特徴とする請求項３に記載の認証通信システム。

【請求項９】　前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

前記記録媒体は、

生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号することを特徴とする請求項３に記載の認証通信システム。

【請求項１０】　前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

コンテンツ鍵を取得するコンテンツ鍵取得部と、

取得したコンテンツ鍵に第１暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第１暗号部と、

生成された前記暗号化コンテンツ鍵に第２暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第２暗号化部と、
前記コンテンツ鍵を用いて、取得した前記デジタル情報に第２暗号アルゴリズムを施して暗号化デジタル情報を生成する第３暗号部とを含み、
前記記録媒体は、
生成された前記二重暗号化コンテンツ鍵に第１復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、
前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含むことを特徴とする請求項３に記載の認証通信システム。
【請求項１１】　デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムで用いられる認証通信方法であって、
前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証ステップと、
前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証ステップと、
前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする認証通信方法。
【請求項１２】　デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記認証通信プログラムは、
前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証ステップと、
前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証ステップと、
前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする記録媒体。
【請求項１３】　請求項１に記載の認証通信システムを構成するアクセス装置。
【請求項１４】　請求項２に記載の認証通信システムを構成するアクセス装置。
【請求項１５】　請求項１に記載の認証通信システムを構成する記録媒体。
【請求項１６】　請求項３に記載の認証通信システムを構成する記録媒体。
【請求項１７】　デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムであって、
前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証ステップと、
前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証ステップと、
前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする認証通信プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタル著作物を機器と記録媒体との間で転送する場合において、機器と記録媒体との間で、相互に正当性を認証する技術に関する。
【０００２】
【従来の技術】近年、デジタル情報圧縮技術の進展と、インターネットに代表されるグローバルな通信インフラの爆発的な普及によって、音楽、画像、映像、ゲームなどの著作物をデジタル著作物として通信回線を介して各家庭に配信することが実現されている。
【０００３】デジタル著作物の著作権者の権利や、流通業者の利益を保護するための流通配信システムを確立す

るために、通信の傍受、盗聴、なりすましなどによる著作物の不正な入手や、受信したデータを記録している記録媒体からの違法な複製、違法な改竄などの不正行為を防止することが課題となっており、正規のシステムかどうかの判別を行ったり、データスクランブルを行う暗号及び認証などの著作物保護技術が必要とされている。

【０００４】著作物保護技術については、従来より様々なものが知られており、代表的なものとして、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換を行って、相互に正当性を認証しあい、正当である場合のみ、アクセスを許可するチャレンジレスポンス型の相互認証技術がある。

【０００５】

【発明が解決しようとする課題】しかしながら、例えば、相互認証を正規な機器を用いて行った後に、正当機器になりすまして、機密データ記憶領域にアクセスすることにより、機密データを不正に入手する行為が考えられる。そこで本発明はかかる問題点に鑑みてなされたものであり、機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置、記録媒体、認証通信システム、認証通信方法、認証通信プログラムを記録している記録媒体及び認証通信プログラムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記の目的を達成するために、本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

【０００７】ここで、前記第１認証フェーズにおいて、前記アクセス装置は、前記領域を示すアクセス情報を取得するアクセス情報取得部と、乱数を取得する乱数取得部と、取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、生成した乱数化アクセス情報に暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、前記記録媒体は、生成された攪乱化アクセス情報から応答値を生成する応答値生成部とを含み、前記アクセス装置は、生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う認証部を含むように構成してもよい。

【０００８】ここで、前記転送フェーズにおいて、前記記録媒体は、生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化アクセス情報を生成する復号部と、伝送された乱数化アクセス情報からアクセス情報を分離する分離部とを含むように構成してもよい。ここで、前記第１認証フェーズにおいて、前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、乱数を取得するように構成してもよい。

【０００９】ここで、前記第１認証フェーズにおいて、前記アクセス装置は、さらに、前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きするように構成してもよい。ここで、前記第１認証フェーズにおいて、前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した乱数種に基づいて乱数を生成することにより、乱数を取得するように構成してもよい。

【００１０】ここで、前記第１認証フェーズにおいて、前記アクセス装置は、さらに、生成された前記乱数を乱数種として前記乱数種記憶部に上書きするように構成してもよい。ここで、前記転送フェーズにおいて、前記領域にデジタル情報を記録している記録媒体は、前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、前記領域からデジタル情報を読み出す前記アクセス装置は、生成された暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成する復号部を含み、前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号するように構成してもよい。

【００１１】ここで、前記転送フェーズにおいて、前記領域へデジタル情報を書き込む前記アクセス装置は、デジタル情報を取得するデジタル情報取得部と、取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、前記記録媒体は、生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号するように構成してもよい。

【００１２】ここで、前記転送フェーズにおいて、前記領域へデジタル情報を書き込む前記アクセス装置は、デジタル情報を取得するデジタル情報取得部と、コンテン

ツ鍵を取得するコンテンツ鍵取得部と、取得したコンテンツ鍵に第１暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第１暗号部と、生成された前記暗号化コンテンツ鍵に第２暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第２暗号化部と、前記コンテンツ鍵を用いて、取得した前記デジタル情報に第２暗号アルゴリズムを施して暗号化デジタル情報を生成する第３暗号部とを含み、前記記録媒体は、生成された前記二重暗号化コンテンツ鍵に第１復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含むように構成してもよい。

【００１３】

【発明の実施の形態】本発明に係る一つの実施の形態としての認証通信システム１００について説明する。

１．認証通信システム１００の外観と利用形態

認証通信システム１００の具体的な構成例としての認証通信システム３０及び３１の外観図を図１（ａ）及び（ｂ）に示す。

【００１４】図１（ａ）に示すように、認証通信システム３０は、パーソナルコンピュータとメモリカード２０から構成される。パーソナルコンピュータは、ディスプレイ部、キーボード、スピーカ、マイクロプロセッサ、ＲＡＭ、ＲＯＭ、ハードディスクユニットなどを備えており、通信回線を経由してインターネットに代表されるネットワークに接続されている。メモリカード２０は、メモリカード挿入口から挿入され、パーソナルコンピュータに装着される。

【００１５】図１（ｂ）に示すように、認証通信システム３１は、ヘッドホンステレオ、メモリカード２０及びヘッドホンから構成される。メモリカード２０は、ヘッドホンステレオのメモリカード挿入口から挿入されて、ヘッドホンステレオに装着される。ヘッドホンステレオは、上面に複数の操作ボタンが配置されており、別の側面にヘッドホンが接続されている。

【００１６】利用者は、メモリカード２０をパーソナルコンピュータに装着し、インターネットを経由して、外部のＷｅｂサーバ装置から音楽などのデジタル著作物を取り込み、取り込んだデジタル著作物をメモリカード２０に書き込む。次に、利用者は、デジタル著作物の記録されているメモリカード２０をヘッドホンステレオに装着し、メモリカード２０に記録されているデジタル著作物をヘッドホンステレオにより再生して、楽しむ。

【００１７】ここで、パーソナルコンピュータとメモリカード２０との間において、また、ヘッドホンステレオとメモリカード２０との間において、チャレンジレスポンス型の認証プロトコルによる各機器の正当性の認証を行い、相互に正当な機器であることが認証された場合にのみ、各機器間でデジタル著作物の転送が行われる。

２．認証通信システム１００の構成

認証通信システム１００は、図２に示すように、リーダライタ装置１０及びメモリカード２０から構成される。ここで、リーダライタ装置１０は、図１（ａ）及び（ｂ）に示すパーソナルコンピュータ及びヘッドホンステレオに相当する。

【００１８】２．１　リーダライタ装置１０の構成

リーダライタ装置１０は、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、暗号復号部１０９、データ記憶部１１０及び入出力部１１１から構成されている。

【００１９】リーダライタ装置１０は、具体的には、マイクロプロセッサ、ＲＡＭ、ＲＯＭその他を備え、ＲＯＭなどにコンピュータプログラムが記録されており、マイクロプロセッサは、前記コンピュータプログラムに従って動作する。

（１）入出力部１１１

入出力部１１１は、利用者の操作を受け付けて、メモリカード２０のデータ記憶部２０９に記憶されている音楽情報にアクセスするためのアクセス情報を生成する。アクセス情報は、図３に示すように、３２ビット長であり、メモリカード２０のデータ記憶部の領域のアドレスを示すアドレス情報と、前記領域のサイズを示すサイズ情報とから構成される。アドレス情報は、２４ビット長であり、サイズ情報は、８ビット長である。

【００２０】また、入出力部１１１は、データ記憶部１１０から音楽情報ＣＴを読み出し、読み出した音楽情報ＣＴを音声信号に変換して出力する。また、入出力部１１１は、利用者の操作を受け付けて、外部から音楽情報ＣＴを取得し、取得した音楽情報ＣＴをデータ記憶部１１０へ書き込む。

（２）アクセス情報記憶部１０１

アクセス情報記憶部１０１は、具体的には、半導体メモリから構成され、アクセス情報を記憶する領域を備えている。

【００２１】（３）乱数種記憶部１０２

乱数種記憶部１０２は、具体的には、半導体メモリから構成され、図３に示すような６４ビット長の乱数種をあらかじめ記憶している。乱数種は、装置の製造時に記録される。乱数種記憶部１０２は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【００２２】（４）合成部１０３

合成部１０３は、アクセス情報記憶部１０１からアクセス情報を読み出し、乱数種記憶部１０２から乱数種を読み出す。次に、図３に示すように、読み出した前記アクセス情報と、読み出した前記乱数種の下位３２ビットと

を結合して、６４ビット長の乱数化アクセス情報を生成する。生成した乱数化アクセス情報を暗号化部１０５へ出力する。

【００２３】（５）共通鍵記憶部１０４

共通鍵記憶部１０４は、具体的には、半導体メモリから構成され、５６ビット長の共通鍵ＵＫを記憶する領域を備えている。リーダライタ装置１０は、メモリカード２０から共通鍵記憶部２０１に記憶されている共通鍵ＵＫを秘密に取得し、共通鍵記憶部１０４は、取得した共通鍵ＵＫを記憶する。

【００２４】共通鍵記憶部１０４は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

（６）暗号化部１０５

暗号化部１０５は、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、合成部１０３から乱数化アクセス情報を受け取る。次に、暗号化部１０５は、共通鍵ＵＫを用いて、受け取った乱数化アクセス情報に暗号アルゴリズムＥ１を施して暗号化アクセス情報Ｒ１を生成する。ここで、暗号化部１０５は、暗号アルゴリズムＥ１として、

（式１）　Ｖ２′＝Ｆ１（Ｒ１、ＵＫ）＝ＳＨＡ（Ｒ１＋ＵＫ）

ここで、関数Ｆ１（ａ、ｂ）は、一例として、ａとｂとを結合し、その結合結果に対してＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）を施す関数である。なお、＋は、結合を示す演算子である。

【００２７】相互認証部１０７は、相互認証部２０７から応答値Ｖ２を受け取る。次に、相互認証部１０７は、Ｖ２とＶ２′とが一致するか否かを判断し、一致しない場合には、メモリカード２０が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。

（式２）　Ｖ１＝Ｆ２（Ｒ２、ＵＫ）＝ＳＨＡ（Ｒ２＋ＵＫ）

（９）時変鍵生成部１０８

時変鍵生成部１０８は、メモリカード２０が正当な装置であると認定され、動作の実行を許可される場合に、暗

（式３）　ＶＫ＝Ｆ３（Ｒ１、Ｒ２）＝ＳＨＡ（Ｒ１＋Ｒ２）

次に、時変鍵生成部１０８は、生成した時変鍵ＶＫを暗号復号部１０９へ出力する。

【００２９】（１０）暗号復号部１０９

暗号復号部１０９は、時変鍵生成部１０８から時変鍵ＶＫを受け取る。暗号復号部１０９は、暗号復号部２１０から暗号化音楽情報ＥｎｃＣＴを受け取り、前記時変鍵ＶＫを用いて、暗号化音楽情報ＥｎｃＣＴに復号アルゴリズムＤ３を施して音楽情報ＣＴを生成し、生成した音楽情報ＣＴをデータ記憶部１１０へ書き込む。

【００３０】ここで、暗号復号部１０９は、復号アルゴリズムＥ３として、ＤＥＳを用いる。また、暗号復号部１０９は、データ記憶部１１０から音楽情報ＣＴを読み出し、前記時変鍵ＶＫを用いて、音楽情報ＣＴに暗号アルゴリズムＥ２を施して暗号化音楽情報ＥｎｃＣＴを生成し、生成した暗号化音楽情報ＥｎｃＣＴを暗号復号部２１０へ出力する。

ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を用いる。

【００２５】次に、暗号化部１０５は、生成した暗号化アクセス情報Ｒ１を、相互認証部１０７と、乱数種更新部１０６と、時変鍵生成部１０８とへ出力する。また、生成した暗号化アクセス情報Ｒ１を、メモリカード２０の復号化部２０５と、相互認証部２０７と、時変鍵生成部２０８とへ出力する。このようにして生成された暗号化アクセス情報Ｒ１は、アクセス情報に撹乱（ｓｃｒａｍｂｌｅ）処理を施して得られる撹乱化情報である。

【００２６】（７）乱数種更新部１０６

乱数種更新部１０６は、暗号化部１０５から暗号化アクセス情報Ｒ１を受け取り、受け取った暗号化アクセス情報Ｒ１を新たな乱数種として乱数種記憶部１０２へ上書きする。

（８）相互認証部１０７

相互認証部１０７は、暗号化アクセス情報Ｒ１を受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、受け取ったＲ１と共通鍵ＵＫとを用いて、式１により、応答値Ｖ２′を算出する。

一致する場合には、相互認証部１０７は、メモリカード２０が正当な装置であると認定し、他の構成部に対して以降の動作の実行を許可する。

【００２８】また、相互認証部１０７は、乱数生成部２０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２と、前記共通鍵ＵＫとを用いて、式２により、応答値Ｖ１を算出し、算出した応答値Ｖ１を相互認証部２０７へ出力する。

号化アクセス情報Ｒ１と乱数Ｒ２とを受け取り、Ｒ１とＲ２とから、式３を用いて時変鍵ＶＫを生成する

【００３１】ここで、暗号復号部１０９は、暗号アルゴリズムＥ２として、ＤＥＳを用いる。

（１１）データ記憶部１１０

データ記憶部１１０は、具体的には、半導体メモリから構成され、音楽情報ＣＴを記憶する領域を備えている。

【００３２】２．２　メモリカード２０

メモリカード２０は、共通鍵記憶部２０１、乱数種記憶部２０２、乱数種更新部２０３、乱数生成部２０４、復号化部２０５、分離部２０６、相互認証部２０７、時変鍵生成部２０８、データ記憶部２０９及び暗号復号部２１０から構成されている。

【００３３】（１）共通鍵記憶部２０１

共通鍵記憶部２０１は、具体的には、半導体メモリから構成され、５６ビット長の共通鍵ＵＫを記憶している。

共通鍵ＵＫは、メモリカード２０の製造時に記録される。共通鍵記憶部２０１は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【００３４】（２）乱数種記憶部２０２

乱数種記憶部２０２は、具体的には、半導体メモリから構成され、６４ビット長の乱数種をあらかじめ記憶している。乱数種は、メモリカード２０の製造時に記録される。乱数種記憶部２０２は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

【００３５】（３）乱数生成部２０４

乱数生成部２０４は、乱数種記憶部２０２から乱数種を読み出し、読み出した乱数種を用いて６４ビット長の乱数Ｒ２を生成し、生成した乱数Ｒ２を乱数種更新部２０３と、相互認証部２０７と、時変鍵生成部２０８とへ出力し、生成した乱数Ｒ２をリーダライタ装置１０の相互認証部１０７と、時変鍵生成部１０８とへ出力する。

【００３６】（４）乱数種更新部２０３

乱数種更新部２０３は、乱数生成部２０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２を新たな乱数種として乱数種記憶部２０２へ上書きする。

（式４）Ｖ２＝Ｆ１（Ｒ１、ＵＫ）＝ＳＨＡ（Ｒ１＋ＵＫ）

ここで、Ｆ１は、式１に示すＦ１と同じ関数であればよい。

【００３９】また、相互認証部２０７は、乱数生成部２

（式５）Ｖ１′＝Ｆ２（Ｒ２、ＵＫ）＝ＳＨＡ（Ｒ２＋ＵＫ）

ここで、Ｆ２は、式２に示すＦ２と同じ関数であればよい。

【００４０】次に、相互認証部２０７は、相互認証部１０７からＶ１を受け取り、Ｖ１とＶ１′とが一致するか否かを判断し、一致しない場合には、リーダライタ装置１０が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部２０７は、リーダライタ装置１０が正当な装置で

（式６）　ＶＫ＝Ｆ３（Ｒ１、Ｒ２）＝ＳＨＡ（Ｒ１＋Ｒ２）

ここで、Ｆ３は、式３に示す関数Ｆ３と同じである。

【００４２】次に、時変鍵生成部２０８は、生成した時変鍵ＶＫを暗号復号部２１０へ出力する。

（９）データ記憶部２０９

データ記憶部２０９は、具体的には、半導体メモリから構成され、音楽情報ＣＴを記憶する領域を備えている。

【００４３】（１０）暗号復号部２１０

暗号復号部２１０は、時変鍵生成部２０８から時変鍵ＶＫを受け取る。暗号復号部２１０は、暗号復号部１０９から暗号化音楽情報ＥｎｃＣＴを受け取り、前記時変鍵ＶＫを用いて、暗号化音楽情報ＥｎｃＣＴに復号アルゴリズムＤ２を施して音楽情報ＣＴを生成し、生成した音楽情報ＣＴをデータ記憶部２０９の前記アクセス情報により示される領域へ書き込む。

（５）復号化部２０５

復号化部２０５は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、暗号化部１０５から暗号化アクセス情報Ｒ１を受け取る。次に、読み出した共通鍵ＵＫを用いて、受け取った暗号化アクセス情報Ｒ１に、復号アルゴリズムＤ１を施して、乱数化アクセス情報を生成し、生成した乱数化アクセス情報を分離部２０６へ出力する。

【００３７】ここで、復号化部２０５は、復号アルゴリズムＤ１として、ＤＥＳを用いる。復号アルゴリズムＤ１は、暗号アルゴリズムＥ１により生成された暗号文を復号する。

（６）分離部２０６

分離部２０６は、復号化部２０５から乱数化アクセス情報を受け取り、受け取った乱数化アクセス情報から、その上位３２ビットのデータをアクセス情報として分離し、アクセス情報をデータ記憶部２０９へ出力する。

【００３８】（７）相互認証部２０７

相互認証部２０７は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、暗号化アクセス情報Ｒ１を受け取り、受け取ったＲ１と共通鍵ＵＫとを用いて、式４により、応答値Ｖ２を算出し、算出したＶ２をリーダライタ装置１０の相互認証部１０７へ出力する。

０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２と、前記共通鍵ＵＫとを用いて、式５により、応答値Ｖ１′を算出する。

あると認定し、他の構成部に対して以降の動作の実行を許可する。

【００４１】（８）時変鍵生成部２０８

時変鍵生成部２０８は、リーダライタ装置１０が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報Ｒ１と乱数Ｒ２とを受け取り、Ｒ１とＲ２とから、式６を用いて時変鍵ＶＫを生成する

【００４４】ここで、暗号復号部２１０は、復号アルゴリズムＤ２として、ＤＥＳを用いる。復号アルゴリズムＤ２は、暗号アルゴリズムＥ２により生成された暗号文を復号する。また、暗号復号部２１０は、データ記憶部２０９の前記アクセス情報により示される領域から音楽情報ＣＴを読み出し、前記時変鍵ＶＫを用いて、音楽情報ＣＴに暗号アルゴリズムＥ３を施して暗号化音楽情報ＥｎｃＣＴを生成し、生成した暗号化音楽情報ＥｎｃＣＴを暗号復号部１０９へ出力する。

【００４５】ここで、暗号復号部２１０は、暗号アルゴリズムＥ３として、ＤＥＳを用いる。復号アルゴリズムＤ３は、暗号アルゴリズムＥ３により生成された暗号文を復号する。

３．認証通信システム１００の動作

（１）読み出し動作

認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０の動作について、図４～図５に示すフローチャートを用いて説明する。

【００４６】なお、ここでは、リーダライタ装置１０は、図１（ｂ）に示すヘッドホンステレオのように、メモリカードに記憶されている情報を読み出す装置であると想定して説明する。合成部１０３は、乱数種記憶部１０２から乱数種を読み出し、アクセス情報記憶部１０１からアクセス情報を読み出し、読み出した前記乱数種と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成し（ステップＳ１０１）、暗号化部は、共通鍵記憶部１０４から共通鍵を読み出し、読み出した前記共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報Ｒ１を生成し（ステップＳ１０２）、相互認証部１０７は、Ｖ２′＝Ｆ１（Ｒ１）を算出し（ステップＳ１０３）、乱数種更新部１０６は、生成された乱数化アクセス情報を新たな乱数種として乱数種記憶部１０２に上書きする（ステップＳ１０４）。

【００４７】暗号化部１０５は、生成した暗号化アクセス情報Ｒ１をメモリカード２０へ出力し、メモリカードの相互認証部２０７は、暗号化アクセス情報Ｒ１を受け取る（ステップＳ１０５）。相互認証部２０７は、Ｖ２＝Ｆ１（Ｒ１）を算出し（ステップＳ１０６）、Ｖ２をリーダライタ装置１０の相互認証部１０７へ出力し、相互認証部１０７は、Ｖ２を受け取る（ステップＳ１０７）。

【００４８】相互認証部１０７は、Ｖ２とＶ２′とが一致するか否かを判断し、一致しない場合には（ステップＳ１０８）、メモリカード２０が不正な装置であると認定し、以後の動作を中止する。一致する場合には（ステップＳ１０８）、相互認証部１０７は、メモリカード２０が正当な装置であると認定し、メモリカード２０の乱数生成部２０４は、乱数種記憶部２０２から乱数種を読み出し、読み出した乱数種を用いて乱数Ｒ２を生成し（ステップＳ１０９）、相互認証部２０７は、Ｖ１′＝Ｆ２（Ｒ２）を算出し（ステップＳ１１０）、乱数種更新部２０３は、生成された乱数Ｒ２を新たに乱数種として乱数種記憶部２０２に上書きする（ステップＳ１１１）。次に、乱数生成部２０４は、生成した乱数Ｒ２をリーダライタ装置１０の相互認証部１０７へ出力し、相互認証部１０７は、乱数Ｒ２を受け取り（ステップＳ１１２）、相互認証部１０７は、Ｖ１＝Ｆ２（Ｒ２）を生成し（ステップＳ１１３）、生成したＶ１をメモリカード２０の相互認証部２０７へ出力し、相互認証部２０７は、Ｖ１を受け取る（ステップＳ１１４）。

【００４９】次に、相互認証部２０７相互認証部２０７は、Ｖ１とＶ１′とが一致するか否かを判断し、一致しない場合には（ステップＳ１１５）、リーダライタ装置１０が不正な装置であると認定し、以後の動作を中止する。一致する場合には（ステップＳ１１５）、相互認証部２０７は、リーダライタ装置１０が正当な装置であると認定し、リーダライタ装置１０の時変鍵生成部１０８は、Ｒ１とＲ２とを用いて時変鍵ＶＫを生成する（ステップＳ１２１）。メモリカード２０の復号化部２０５は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いてＲ１を復号して乱数化アクセス情報を生成し（ステップＳ１２２）、分離部２０６は、乱数化アクセス情報からアクセス情報を分離し（ステップＳ１２３）、時変鍵生成部２０８は、Ｒ１とＲ２とを用いて時変鍵ＶＫを生成し（ステップＳ１２４）、暗号復号部２１０は、アクセス情報により示されるデータ記憶部２０９の領域から音楽情報ＣＴを読み出し（ステップＳ１２５）、暗号復号部２１０は、生成された時変鍵ＶＫを用いて読み出した前記音楽情報ＣＴを暗号化して暗号化音楽情報ＥｎｃＣＴを生成し（ステップＳ１２６）、生成した暗号化音楽情報ＥｎｃＣＴをリーダライタ装置１０の暗号復号部１０９へ出力する（ステップＳ１２７）。

【００５０】暗号復号部１０９は、時変鍵ＶＫを用いて暗号化音楽情報ＥｎｃＣＴを復号して音楽情報ＣＴを生成してデータ記憶部１１０へ書き込み（ステップＳ１２８）、入出力部１１１は、音楽情報ＣＴをデータ記憶部１１０から読み出し、読み出した音楽情報ＣＴを音声信号に変換して出力する（ステップＳ１２９）。

（２）書き込み動作

認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０の動作について、図６に示すフローチャートを用いて説明する。

【００５１】ここでは、リーダライタ装置１０は、図１（ａ）に示すパーソナルコンピュータのように、メモリカードに情報を書き込む装置であると想定して説明する。また、読み出し動作と書き込み動作は類似しているので、相違点のみについて説明する。図４～図５のフローチャートのステップＳ１２５～Ｓ１２９を、図６に示すステップに置き換えると認証通信システム１００の書き込み動作となる。

【００５２】暗号復号部１０９は、データ記憶部１１０から音楽情報ＣＴを読み出し（ステップＳ１３１）、時変鍵ＶＫを用いて読み出した音楽情報ＣＴを暗号化して暗号化音楽情報ＣＴを生成し（ステップＳ１３２）、生成した暗号化音楽情報ＣＴをメモリカード２０の暗号復号部２１０へ出力し、暗号復号部２１０は、暗号化音楽情報ＣＴを受け取る（ステップＳ１３３）。

【００５３】暗号復号部２１０は、暗号化音楽情報ＥｎｃＣＴを時変鍵ＶＫを用いて復号して音楽情報ＣＴを生成し（ステップＳ１３４）、生成した音楽情報ＣＴを前記アクセス情報で示されるデータ記憶部２０９内の領域に書き込む（ステップＳ１３５）。

４．まとめ

以上説明したように、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

【００５４】また、仮に機密データ記憶領域にアクセスするための情報が、不正ななりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が確立しないので、機密データ記憶領域にアクセスできないようにすることができる。また、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

【００５５】５．認証通信システム１００ａ

認証通信システム１００の変形例としての認証通信システム１００ａについて説明する。

５．１　認証通信システム１００ａの構成

認証通信システム１００ａは、図７に示すように、リーダライタ装置１０ａとメモリカード２０とから構成される。

【００５６】メモリカード２０は、図２に示すメモリカード２０と同じであるので、ここでは、説明を省略する。リーダライタ装置１０ａは、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、暗号復号部１０９、データ記憶部１１０、入出力部１１１及び乱数生成部１１２から構成されている。

【００５７】リーダライタ装置１０との相違点を中心として、以下に説明する。その他の点については、リーダライタ装置１０と同じであるので、説明を省略する。

（１）乱数生成部１１２

乱数生成部１１２は、乱数種記憶部１０２から乱数種を読み出し、読み出した乱数種を用いて６４ビット長の乱数を生成し、生成した乱数を合成部１０３と乱数種更新部１０６とへ出力する。

【００５８】（２）乱数種更新部１０６

乱数種更新部１０６は、乱数生成部１１２から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部１０２へ上書きする。

（３）合成部１０３

合成部１０３は、乱数生成部１１２から乱数を受け取り、アクセス情報記憶部１０１からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する。

【００５９】５．２　認証通信システム１００ａの動作

認証通信システム１００ａの動作について、図８に示すフローチャートを用いて説明する。乱数生成部１１２は、乱数種記憶部１０２から乱数種を読み出し（ステップＳ２０１）、読み出した乱数種を用いて６４ビット長の乱数を生成し（ステップＳ２０２）、乱数種更新部１０６は、乱数生成部１１２から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部１０２へ上書きする（ステップＳ２０３）。次に、合成部１０３は、乱数生成部１１２から乱数を受け取り、アクセス情報記憶部１０１からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する（ステップＳ２０４）。

【００６０】次に、図４のステップＳ１０２へ続く。以下は、認証通信システム１００の動作と同じであるので、説明を省略する。

５．３　まとめ

以上説明したように、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

【００６１】６．認証通信システム１００ｂ

認証通信システム１００ａの変形例としての認証通信システム１００ｂについて説明する。

６．１　認証通信システム１００ｂの構成

認証通信システム１００ｂは、図９に示すように、リーダライタ装置１０ｂとメモリカード２０ｂとから構成される。

【００６２】（１）リーダライタ装置１０ｂの構成

リーダライタ装置１０ｂは、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、データ記憶部１１０、入出力部１１１、乱数生成部１１２、コンテンツ鍵生成部１１３、暗号化部１１４、コンテンツ付加情報記憶部１１５、暗号復号部１１６及び暗号化部１１７から構成されている。

【００６３】以下において、リーダライタ装置１０ａとの相違点を中心として説明する。その他の点については、リーダライタ装置１０ａと同じであるので、説明を省略している。

（ａ）入出力部１１１

入出力部１１１は、利用者の操作によりコンテンツ付加情報の入力を受け付け、受け付けたコンテンツ付加情報をコンテンツ付加情報記憶部１１５に書き込む。

【００６４】ここで、コンテンツ付加情報の一例は、コンテンツの再生回数、使用期間であり、コンテンツ付加情報は、８ビット長である。また、入出力部１１１は、利用者の操作によりコンテンツデータＣＤを取得し、取得したコンテンツデータＣＤをデータ記憶部１１０に書き込む。ここで、コンテンツデータＣＤは、一例として音楽コンテンツ情報である。

【００６５】（ｂ）乱数生成部１１２

乱数生成部１１２は、生成した乱数Ｒ３をコンテンツ鍵生成部１１３へ出力する。

（ｃ）コンテンツ鍵生成部１１３

コンテンツ鍵生成部１１３は、コンテンツ付加情報記憶部１１５からコンテンツ付加情報を読み出し、乱数生成部１１２から乱数Ｒ３を受け取り、乱数Ｒ３と読み出したコンテンツ付加情報を用いて、式７により、コンテンツ鍵ＣＫを生成する。ここで、コンテンツ鍵ＣＫは、６４ビット長である。

（式７）ＣＫ＝Ｆ４（Ｒ３、コンテンツ付加情報）
＝コンテンツ付加情報（８ビット長）＋Ｒ３の下位５６ビット

ここで、＋は、データとデータの結合を示す演算子である。

【００６６】次に、コンテンツ鍵生成部１１３は、生成したコンテンツ鍵ＣＫを暗号化部１１４と、暗号化部１１７とへ出力する。

（ｄ）暗号化部１１４

暗号化部１１４は、コンテンツ鍵生成部１１３からコンテンツ鍵ＣＫを受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ４を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを暗号復号部１１６へ出力する。

【００６７】ここで、暗号化部１１４は、暗号アルゴリズムＥ４として、ＤＥＳを用いる。

（ｅ）暗号復号部１１６

暗号復号部１１６は、暗号化部１１４から暗号化コンテンツ鍵ＥｎｃＣＫを受け取り、受け取った暗号化コンテンツ鍵ＥｎｃＣＫに、時変鍵ＶＫを用いて、暗号アルゴリズムＥ２を施してＥｎｃ（ＥｎｃＣＫ）を生成し、生成したＥｎｃ（ＥｎｃＣＫ）を暗号復号部２１１へ出力する。

【００６８】ここで、暗号復号部１１６は、暗号アルゴリズムＥ２として、ＤＥＳを用いる。

（ｆ）暗号化部１１７

暗号化部１１７は、データ記憶部１１０からコンテンツデータＣＤを読み出し、読み出したコンテンツデータＣＤに、コンテンツ鍵ＣＫを用いて、暗号化アルゴリズムＥ５を施して暗号化コンテンツデータＥｎｃＣＤを生成する。次に、暗号化部１１７は、生成した暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３へ出力する。

【００６９】ここで、暗号化部１１７は、暗号アルゴリズムＥ５として、ＤＥＳを用いる。

（２）メモリカード２０ｂの構成

メモリカード２０ｂは、共通鍵記憶部２０１、乱数種記憶部２０２、乱数種更新部２０３、乱数生成部２０４、復号化部２０５、分離部２０６、相互認証部２０７、時変鍵生成部２０８、暗号復号部２１１、鍵データ記憶部２１２及びデータ記憶部２１３から構成されている。

【００７０】以下において、メモリカード２０との相違点を中心として説明する。その他の点については、メモリカード２０と同じであるので、説明を省略している。

（ａ）時変鍵生成部２０８

時変鍵生成部２０８は、時変鍵ＶＫを暗号復号部２１１へ出力する。

（ｂ）暗号復号部２１１

暗号復号部２１１は、時変鍵生成部２０８から時変鍵ＶＫを受け取り、暗号復号部１１６からＥｎｃ（ＥｎｃＣＫ）を受け取る。

【００７１】次に、暗号復号部２１１は、時変鍵ＶＫを用いてＥｎｃ（ＥｎｃＣＫ）に復号アルゴリズムＤ２を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを前記アクセス情報により示される鍵データ記憶部２１２の領域に書き込む。

（ｃ）鍵データ記憶部２１２

鍵データ記憶部２１２は、暗号化コンテンツ鍵ＥｎｃＣＫを記憶する領域を備える。

【００７２】（ｄ）データ記憶部２１３

データ記憶部２１３は、暗号化コンテンツデータＥｎｃＣＤを受け取り、受け取った暗号化コンテンツデータＥｎｃＣＤを記憶する。

６．２　認証通信システム１００ｂの動作

認証通信システム１００ｂの動作は、認証通信システム１００ａの動作に類似している。ここでは、認証通信システム１００ａとの相違点についてのみ説明する。

【００７３】認証通信システム１００ｂの動作は、認証通信システム１００ａの動作を示すフローチャートのうち、ステップＳ１２１以降を図１０に示すフローチャートに置き換えたフローチャートにより示される。コンテンツ鍵生成部１１３は、コンテンツ付加情報記憶部１１５からコンテンツ付加情報を読み出し（ステップＳ３０１）、乱数生成部１１２は、生成した乱数Ｒ３をコンテンツ鍵生成部１１３へ出力し、コンテンツ鍵生成部１１３は、乱数生成部１１２からＲ３を受け取り、Ｒ３と読み出したコンテンツ付加情報を用いて、コンテンツ鍵ＣＫを生成し、生成したコンテンツ鍵ＣＫを暗号化部１１４と、暗号化部１１７とへ出力し（ステップＳ３０２）、暗号化部１１４は、コンテンツ鍵生成部１１３からコンテンツ鍵ＣＫを受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ４を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを暗号復号部１１６へ出力する（ステップＳ３０３）。次に、暗号復号部１１６は、暗号化コンテンツ鍵ＥｎｃＣＫを受け取り、受け取った暗号化コンテンツ鍵ＥｎｃＣＫに時変鍵ＶＫを用いて暗号アルゴリズムＥ２を施してＥｎｃ（ＥｎｃＣＫ）を生成し（ステップＳ３０４）、暗号復号部１１６は、生成したＥｎｃ（ＥｎｃＣＫ）を暗号復号部

２１１へ出力し、暗号復号部２１１は、Ｅｎｃ（ＥｎｃＣＫ）を受け取り（ステップＳ３０５）、暗号復号部２１１は、Ｅｎｃ（ＥｎｃＣＫ）に時変鍵ＶＫを用いて復号アルゴリズムＤ２を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを前記アクセス情報により示される鍵データ記憶部２１２の領域に書き込む（ステップＳ３０６）。

【００７４】暗号化部１１７は、データ記憶部１１０からコンテンツデータＣＤを読み出し（ステップＳ３０７）、読み出したコンテンツデータＣＤにコンテンツ鍵ＣＫを用いて暗号化アルゴリズムＥ５を施して暗号化コンテンツデータＥｎｃＣＤを生成する（ステップＳ３０８）。暗号化部１１７は、生成した暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３へ出力し、データ記憶部２１３は、暗号化コンテンツデータＥｎｃＣＤを受け取り（ステップＳ３０９）、データ記憶部２１３は、受け取った暗号化コンテンツデータＥｎｃＣＤを記憶する（ステップＳ３１０）。

【００７５】６．３　まとめ

以上説明したように、認証通信システム１００ｂにおいて、コンテンツデータを暗号化するためのコンテンツ鍵を生成するのに、新たな乱数発生機構を必要とせず、アクセス情報の合成に用いる乱数発生機構と共有化できる。

７．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【００７６】（１）上記の実施の形態において、デジタル著作物は、音楽の情報であるとしているが、小説や論文などの文字データ、コンピュータゲーム用のコンピュータプログラムソフトウェア、ＭＰ３などに代表される圧縮された音声データ、ＪＰＥＧなどの静止画像、ＭＰＥＧなどの動画像であるとしてもよい。また、リーダライタ装置は、パーソナルコンピュータに限定されず、上記の様々なデジタル著作物を販売したり配布したりする出力装置であるとしてもよい。また、リーダライタ装置は、ヘッドホンステレオに限定されず、デジタル著作物を再生する再生装置であるとしてもよい。例えば、コンピュータゲーム装置、帯型情報端末、専用装置、パーソナルコンピュータなどであるとしてもよい。また、リーダライタ装置は、上記出力装置と再生装置との両方を兼ね備えているとしてもよい。

【００７７】（２）上記の実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、ＤＥＳを用いるとしているが、他の暗号を用いるとしてもよい。また、上記実施の形態において、ＳＨＡを用いるとしているが、他の一方向性関数を用いるとしてもよい。共通鍵、時変鍵の鍵長は、５６ビットであるとしているが、他の長さの鍵を用いるとしてもよい。

【００７８】（３）上記の実施の形態において、合成部１０３は、アクセス情報と、乱数種の下位３２ビットとを結合して、６４ビット長の乱数化アクセス情報を生成するとしているが、これに限定されない。次のようにしてもよい。合成部１０３は、３２ビットのアクセス情報と、乱数種の下位３２ビットとを１ビットずつ交互に結合して、６４ビット長の乱数化アクセス情報を生成していもよい。また、複数ビットずつ交互に結合してもよい。この場合、分離部２０６は、逆の操作を行うようにする。

【００７９】（４）上記の実施の形態において、メモリカード２０の乱数生成部２０４は、乱数種記憶部２０２に記憶されている乱数種を用いて乱数Ｒ２を生成するとしているが、乱数生成部２０４は、乱数種を乱数Ｒ２として生成してもよい。また、時変鍵生成部１０８、２０８は、Ｒ１及びＲ２を用いて時変鍵を生成するとしているが、応答値を用いるとしてもよい。また、共通鍵ＵＫを絡ませてもよい。

【００８０】（５）認証通信システム１００ｂにおいて、暗号化部１１７は、暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３に書き込むとしているが、暗号化コンテンツデータＥｎｃＣＤを機密データとして扱って、アクセス情報により示される領域に書き込むとしてもよい。また、暗号化コンテンツ鍵ＥｎｃＣＫを機密データとして扱わずに、データ記憶部２１３に書き込むとしてもよい。

【００８１】また、暗号化部１１４及び暗号化部１１７のいずれか一方を無くし、残っている一方により共有化してもよい。

（６）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【００８２】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピー（登録商標）ディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００８３】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサ

は、前記コンピュータプログラムに従って動作するとしてもよい。

【００８４】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（４）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【００８５】８．産業上の利用の可能性

デジタル著作物を出力する出力装置から半導体記録媒体へデジタル著作物を複製する場合において、出力装置と半導体記録媒体とが、相互に正当性を認証する場合に利用することができる。また、デジタル著作物の記録されている半導体記録媒体からデジタル著作物を読み出して再生する場合において、半導体記録媒体と再生装置との間で、各装置が、相互に正当性を認証する場合に利用することができる。

【００８６】

【発明の効果】上記目的を達成するために本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

【００８７】これによって、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。また、仮に、機密データ記憶領域にアクセスするための情報が、不正ななりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が成功しないので、機密データ記憶領域にアクセスできないようにすることができる。

【図面の簡単な説明】

【図１】図１は、認証通信システム１００の具体的な構成例としての認証通信システム３０及び３１の外観を示す。図１（ａ）は、パーソナルコンピュータとメモリカード２０から構成される認証通信システム３０の外観を示し、図１（ｂ）は、ヘッドホンステレオ、メモリカード２０及びヘッドホンから構成される認証通信システム３１の外観を示す。

【図２】図２は、認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０のそれぞれ構成を示すブロック図である。

【図３】図３は、アクセス情報、乱数種及び乱数化アクセス情報のデータ構造を示す。

【図４】図４は、認証通信システム１００の動作を示すフローチャートであり、特に、メモリカードに記憶されている情報を読み出す場合を想定したものである。図５に続く。

【図５】図５は、認証通信システム１００の動作を示すフローチャートである。図４から続く。

【図６】図６は、認証通信システム１００の動作を示すフローチャートであり、特に、リーダライタ装置１０は、メモリカードに情報を書き込む装置であると想定した場合のものである。

【図７】図７は、別の実施の形態としての、認証通信システム１００ａの構成を示すブロック図である。

【図８】図８は、認証通信システム１００ａに固有の動作を示すフローチャートである。

【図９】図９は、別の実施の形態としての、認証通信システム１００ｂの構成を示すブロック図である。

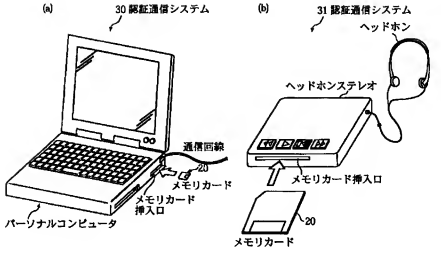
【図１０】図１０は、認証通信システム１００ｂに固有の動作を示すフローチャートである。

【符号の説明】

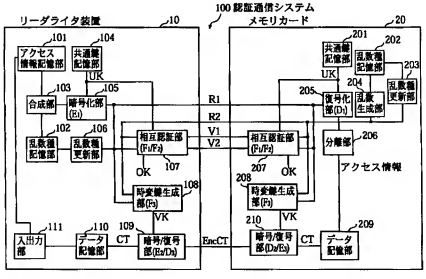
１００　認証通信システム
１０　リーダライタ装置
１０１　アクセス情報記憶部
１０２　乱数種記憶部
１０３　合成部
１０４　共通鍵記憶部
１０５　暗号化部
１０６　乱数種更新部
１０７　相互認証部
１０８　時変鍵生成部
１０９　暗号復号部
１１０　データ記憶部
１１１　入出力部
２０　メモリカード
２０１　共通鍵記憶部
２０２　乱数種記憶部
２０３　乱数種更新部
２０４　乱数生成部
２０５　復号化部
２０６　分離部
２０７　相互認証部
２０８　時変鍵生成部

２０９　データ記憶部　　２１０　暗号復号部

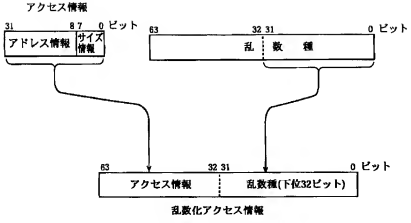
【図１】



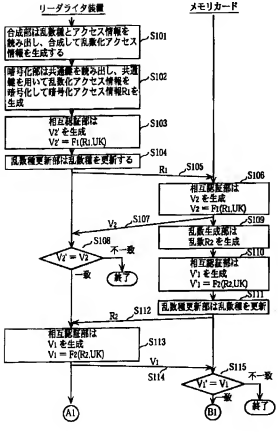
【図２】



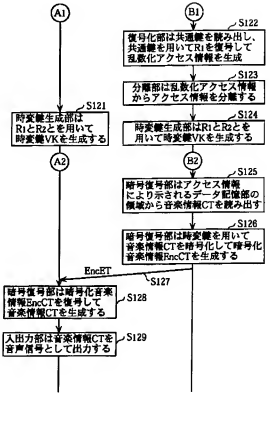
【図３】


アクセス情報
31
8 7
0 ビット
アドレス情報
サイズ情報
63
32 31
0 ビット
乱数種
63
32 31
0 ビット
アクセス情報
乱数種(下位32ビット)
乱数化アクセス情報

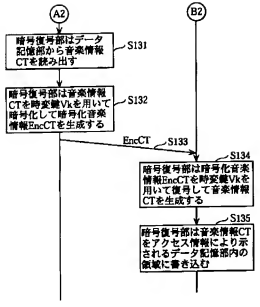
【図４】


リーダライタ装置
メモリカード
合成部は乱数種とアクセス情報を読み出し、合成して乱数化アクセス情報を生成する
S101
暗号化部は共通鍵を読み出し、共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報R1を生成
S102
相互認証部は V2' を生成 V2' = F1(R1,UK)
S103
乱数種更新部は乱数種を更新する
S104
R1
S105
相互認証部は V2 を生成 V2 = F1(R1,UK)
S106
V2
S107
S109
乱数生成部は乱数R2 を生成
S108
V2' = V2
不一致
一致
終了
S110
相互認証部は V1' を生成 V1' = F2(R2,UK)
S111
乱数種更新部は乱数種を更新
R2
S112
相互認証部は V1 を生成 V1 = F2(R2,UK)
S113
V1
S114
S115
V1' = V1
不一致
一致
終了
A1
B1

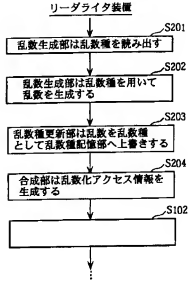
【図５】


A1
時変鍵生成部は R1とR2とを用いて 時変鍵VKを生成する
S121
A2
EncET
暗号復号部は暗号化音楽情報EncCTを復号して音楽情報CTを生成する
S128
入出力部は音楽情報CTを音声信号として出力する
S129
B1
復号化部は共通鍵を読み出し、共通鍵を用いてR1を復号して乱数化アクセス情報を生成
S122
分離部は乱数化アクセス情報からアクセス情報を分離する
S123
時変鍵生成部はR1とR2とを用いて時変鍵VKを生成する
S124
B2
暗号復号部はアクセス情報により示されるデータ記憶部の領域から音楽情報CTを読み出す
S125
暗号復号部は時変鍵を用いて音楽情報CTを暗号化して暗号化音楽情報EncCTを生成する
S126
S127

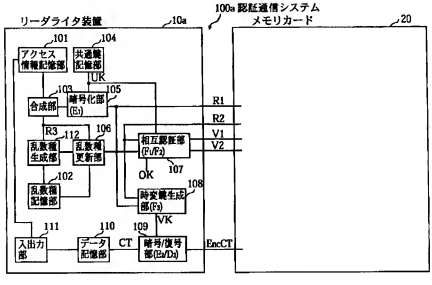
【図６】


AZ
BZ
暗号復号部はデータ記憶部から音楽情報CTを読み出す
S131
暗号復号部は音楽情報CTを時変鍵Vkを用いて暗号化して暗号化音楽情報EncCTを生成する
S132
EncCT
S133
S134
暗号復号部は暗号化音楽情報EncCTを時変鍵Vkを用いて復号して音楽情報CTを生成する
S135
暗号復号部は音楽情報CTをアクセス情報により示されるデータ記憶部内の領域に書き込む

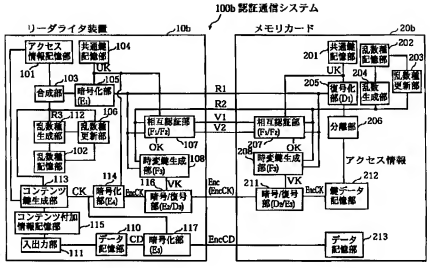
【図８】


リーダライタ装置
S201
乱数生成部は乱数種を読み出す
S202
乱数生成部は乱数種を用いて乱数を生成する
S203
乱数種更新部は乱数を乱数種として乱数種記憶部へ上書きする
S204
合成部は乱数化アクセス情報を生成する
S102

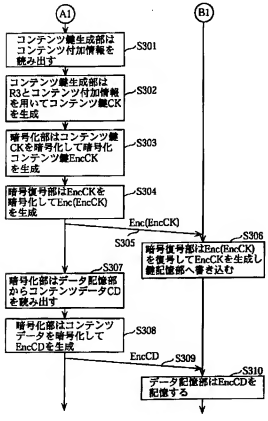
【図７】


100a 認証通信システム
リーダライタ装置
10a
メモリカード
20
101
アクセス情報記憶部
104
共通鍵記憶部
UK
103
合成部
105
暗号化部 (Eb)
R1
R2
R3
112
106
乱数種生成部
乱数種更新部
相互認証部 (Fv/Ff2)
V1
V2
102
OK
107
乱数種記憶部
時変鍵生成部(Ff)
108
VK
111
110
109
入出力部
データ記憶部
CT
暗号/復号部(Eb/Db)
EncCT

【図９】


100b 認証通信システム
リーダライタ装置
10b
メモリカード
20b
アクセス情報記憶部
101
共通鍵記憶部
104
UK
103
105
合成部
暗号化部(Ea)
R1
R2
R3
112
106
乱数値生成部
乱数値更新部
乱数値記憶部
102
相互認証部(Fv/Fa)
V1
V2
OK
107
時変鍵生成部(Fs)
108
113
114
116
VK
Enc(EncCK)
コンテンツ鍵生成部
CK
暗号化部(Ea)
EncCK
暗号/復号部(Ds/Da)
コンテンツ付加情報記憶部
115
110
117
入出力部
111
データ記憶部
CD
暗号化部(Es)
EncCD
201
共通鍵記憶部
乱数値記憶部
202
203
UK
204
205
復号化部(Dd)
乱数値生成部
乱数値更新部
相互認証部(Fv/Fa)
分離部
206
207
OK
208
時変鍵生成部(Fs)
アクセス情報
211
VK
212
暗号/復号部(Ds/Da)
EncCK
鍵データ記憶部
データ記憶部
213

【図１０】


A1
B1
コンテンツ鍵生成部はコンテンツ付加情報を読み出す
S301
コンテンツ鍵生成部はR3とコンテンツ付加情報を用いてコンテンツ鍵CKを生成
S302
暗号化部はコンテンツ鍵CKを暗号化して暗号化コンテンツ鍵EncCKを生成
S303
暗号復号部はEncCKを暗号化してEnc(EncCK)を生成
S304
Enc(EncCK)
S305
S306
暗号復号部はEnc(EncCK)を復号してEncCKを生成し鍵記憶部へ書き込む
S307
暗号化部はデータ記憶部からコンテンツデータCDを読み出す
暗号化部はコンテンツデータを暗号化してEncCDを生成
S308
EncCD
S309
S310
データ記憶部はEncCDを記憶する

フロントページの続き

(51) Int. Cl. 7		識別記号
Ｇ０９Ｃ	1/00	６６０
Ｈ０４Ｌ	9/08	
	9/10	
	9/32	

Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｋ	19/00	Ｒ
Ｈ０４Ｌ	9/00	６０１Ａ
		６２１Ａ
		６７５Ａ

(72)発明者　関部　勉
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　廣田　照人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　齊藤　義行
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大竹　俊彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム（参考）　5B017 AA03 BA05 BA07 CA14
5B035 AA13 BB09 BC00 CA11
5B058 CA27 KA02 KA04 KA08 KA35
YA20
5J104 AA01 AA07 AA15 AA16 EA06
EA07 JA13 KA02 KA04 KA06
NA02 NA35 NA37